1

Equidistant Linear Network Codes with maximal Error-protection from Veronese Varieties

Johan P. Hansen

***Abstract*—Linear network coding transmits information in terms of a basis of a vector space and the information is received as a basis of a possible altered vectorspace. Ralf Koetter and Frank R. Kschischang [1] introduced a metric on the set af vector-spaces and showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector-space is sufficiently large.**

From the Veronese varieties we construct explicit families of vector-spaces of constant dimension where any pair of distinct vector-spaces are equidistant in the above metric. The parameters of the resulting linear network codes which have maximal error-protection are determined.

***Index Terms*—Algebra, error correction codes, algebraic coding, network information theory, network robustness, Veronese varieties.**

Johan P. Hansen July 9, 2012

A. Notation

- $\mathbb{F}_q$ is the finite field with q elements of characteristic p.
- $k = \overline{\mathbb{F}_q}$ is an algebraic closure of $\mathbb{F}_q$.
- $G(n, N)$ is the Grassmannian of n-dimensional k-linear subspaces of k^N and $G(n, N)(\mathbb{F}_q)$ is its $\mathbb{F}_q$-rational points, i.e. n-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$.
- $\mathcal{V} = \sigma_d(\mathbb{P}^m) \subseteq \mathbb{P}^M$ with $M = \binom{m+d}{m} - 1$ is the Veronese variety, see III.

For generalities on algebric geometry we refer to [2].

I. Linear network coding

In linear network coding transmission is obtained by transmitting a number of packets into the network and each packet is regarded as a vector of length N over a finite field $\mathbb{F}_q$. The packets travel the network through intermediate nodes, each forwarding $\mathbb{F}_q$-linear combinations of the packets it has available. Eventually the receiver tries to infer the originally transmitted packages from the packets that are recieved, see [3] and [4].

All packets are vectors in $\mathbb{F}_q^N$; however Ralf Koetter and Frank R. Kschischang [1] describes a transmission model in terms of linear subspaces of $\mathbb{F}_q^N$ spanned by the packets and they define a fixed dimension *code* as a nonempty subset $\mathcal{C} \subseteq G(n, N)(\mathbb{F}_q)$ of the Grassmannian of n-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$. They endowed the Grassmannian $G(n, N)(\mathbb{F}_q)$ with the metric

$$d(V, U) := \dim_{\mathbb{F}_q}(V + U) - \dim_{\mathbb{F}_q}(U \cap V), \qquad (1)$$

where $U, V \in G(n, N)(\mathbb{F}_q)$.

Johan P. Hansen is with the Department of Mathematics, Aarhus University, Aarhus, Denmark, e-mail: matjph@imf.au.dk.

The size of the code $\mathcal{C} \subseteq G(n, N)(\mathbb{F}_q)$ is denoted by $|\mathcal{C}|$, the minimal distance by

$$D(\mathcal{C}) := \min_{U,V \in \mathcal{C}, U \neq V} d(U, V) \qquad (2)$$

and $\mathcal{C}$ is said to be of type $[N, n, \log_q |\mathcal{C}|, D(\mathcal{C})]$. Its normalized weight is $\lambda = \frac{n}{N}$, its rate is $R = \frac{\log_q(|\mathcal{C}|)}{Nn}$ and its normalized minimal distance is $\delta = \frac{D(\mathcal{C})}{2n}$.

They showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector-space is sufficiently large. Also they obtained Hamming, Gilbert-Varshamov and Singleton coding bounds.

They exhibited linear network codes whose code words are the $\mathbb{F}_q$-rational points on the complements of a hyperplane section of the Grassmannians in their Plücker embedding, however these codes have no error protection. In contrast our linear network codes from the Veronese varieties have in some sense maximal error protection.

II. Linear network codes from the Veronese varities

We obtain linear network codes $\mathcal{C} \subseteq G(n, N)(\mathbb{F}_q)$ of the Grassmannian of n-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$ with *equidistant* code words and with large normalized minimal distance from a geometric construction using the tangent spaces to the d-uple embeddings of projective spaces, see III.

Definition 1. Let $n \geq 2$ and $d \geq 2$ be integers and let $\mathcal{V} = \sigma_d(\mathbb{P}^{n-1})$ be the d-uple embedding of $\mathbb{P}^{n-1}$ in $\mathbb{P}^{N-1}$ with $N = \binom{n-1+d}{n-1}$.

The code $\mathcal{C}_n^d \subseteq G(n, N)(\mathbb{F}_q)$ consists of the n-dimensional affine cones in $\mathbb{F}_q^N$ of the projective tangent spaces T_P to $\mathcal{V} = \sigma_d(\mathbb{P}^{n-1}) \subseteq P^{N-1}$ at the $\mathbb{F}_q$-rational points $P \in \mathcal{V}$:

$$\mathcal{C}_n^d = \{\text{affine cone}\,(\mathrm{T_P}) \subseteq \mathbb{F}_\mathrm{q}^\mathrm{N} |\ \mathrm{P} \in \mathcal{V}(\mathbb{F}_\mathrm{q})\}\ .$$

The codes obtained this way from the tangent spaces to the Veronese varieties are equidistant linear network codes with large minimal distances.

Theorem 2. *Let $\mathcal{C}_n^d \subseteq G(n, N)(\mathbb{F}_q)$ be the codes defined above. The code $\mathcal{C}_n^d$ has the size*

$$|\mathcal{V}(\mathbb{F}_q)| = \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}\ .$$

The codes $\mathcal{C}_n^d$ have equidistant code words. Specifically let U and V be two distinct vector-spaces. Assume that the characteristic p is not a divisor of d, then

i) *if* $d \geq 3$, *then* $d(U,V) = 2n$ *and the codes are of type* $[\binom{n-1+d}{n-1}, n, \log_q \frac{q^n-1}{q-1}, 2n]$ *with normalized minimal distance* $\delta = 1$.

ii) *if* $d = 2$, *then* $d(U,V) = 2n-2$ *and the codes are of type* $[\binom{n-1+d}{n-1}, n, \log_q \frac{q^n-1}{q-1}, 2n-2]$ *with normalized minimal distance* $\delta = 1 - \frac{1}{n}$.

If the characteristic p *is a divisor of* d, *then*

iii) $d(U,V) = 2n-4$ *and the codes are of type* $[\binom{n-1+d}{n-1}, n, \log_q \frac{q^n-1}{q-1}, 2n-4]$ *with normalized minimal distance* $\delta = 1 - \frac{2}{n}$

Proof: The number of $\mathbb{F}_q$-rational points on $\mathbb{P}^{n-1}$ and $\mathcal{V}$ is $\frac{q^n-1}{q-1} = 1+q+\cdots+q^{n-1}$. The claims on the distances follows from Proposition 3 below applied with $m = n-1, N = M-1$ and where U, V are the affine cones of the projective tangent-spaces T_P, T_Q to $\mathcal{V} \subseteq \mathbb{P}^{N-1}$ at P, Q. ∎

III. The d-uple embedding and the Veronese variety

Let $\mathbb{P}^m$ with $m \geq 1$ be the projective m-space over k with homogenous coordinates $X_0, \ldots, X_m$.

For each integer $d \geq 1$, let $X_0^{d_0} X_1^{d_1} \ldots X_m^{d_m}$ with $d_0 + d_1 + \cdots + d_m = d$ be the $\binom{m+d}{d}$ monomials of total degree d in the $m+1$ variables $X_0, \ldots, X_m$. Let $\mathbb{P}^M$ be the projective space with homogenous coordinates $Z_{d_0,\ldots,d_m}$ of dimension $M = \binom{m+d}{d} - 1$.

The d-uple embedding is the mapping

$$\sigma_d : \mathbb{P}^m \to \mathbb{P}^M$$

having the monomials in $X_0, \ldots, X_m$ of degree d as coordinate functions. A point $P = (x_0 : \cdots : x_m) \in \mathbb{P}^m$ is mapped to the point in $\mathbb{P}^M$ with coordinates $z_{d_0,d_1,\ldots,d_m} = x_0^{d_0} x_1^{d_1} \ldots x_m^{d_m}$ obtained by substituting x_i in the monomials $X_0^{d_0} X_1^{d_1} \ldots X_m^{d_m}$.

Its image is the Veronese variety $\mathcal{V} = \sigma_d(\mathbb{P}^m) \subseteq \mathbb{P}^M$ and σ_d is an isomorphism from $\mathbb{P}^m$ to $\mathcal{V}$.

Proposition 3. *Let* P, Q *be two different points on the Veronese variety* $\mathcal{V}$ *and let* T_P *and* T_Q *be the corresponding tangent-spaces to* $\mathcal{V}$ *in* $\mathbb{P}^M$.

Assume that the characteristic p *is not a divisor of* d.

i) *If* $d \geq 3$, *then* $T_P \cap T_Q = \emptyset$,

ii) *If* $d = 2$, *then* $\dim_k(T_P \cap T_Q) = 0$.

If the characteristic p *is a divisor of* d, *then*

iii) $\dim_k(T_P \cap T_Q) = 1$.

Proof: We wil use the fact, that a hyperplane H in $\mathbb{P}^M$ with equation

$$H : \sum_{d_0,\ldots,d_n} a_{d_0,\ldots,d_n} Z_{d_0,\ldots,d_n} = 0 \qquad (3)$$

contains the tanget space T_P of $\mathcal{V}$ if and only if the corresponding degree d hypersurface $\sigma_d^{-1}(H) \subseteq \mathbb{P}^m$ is singular at the point $\sigma_d^{-1}(P) \in \mathbb{P}^m$.

After a possible change of coordinates we can assume that $P = \sigma_d(1:0:0:\cdots:0)$ and $Q = \sigma_d(0:1:0:\cdots:0)$. The conditions that the hyperplane of (3) contains both T_P and T_Q translates to the $2(m+1)$ equations

$$\begin{aligned}
d{\cdot}a_{d,0,0,0\ldots,0} &= 0\\
a_{d-1,1,0,0\ldots,0} &= 0\\
a_{d-1,0,1,0\ldots,0} &= 0\\
a_{d-1,0,0,1\ldots,0} &= 0\\
\vdots &= \vdots\\
a_{d-1,0,0,0\ldots,1} &= 0\\
a_{1,d-1,0,0\ldots,0} &= 0\\
d{\cdot}a_{0,d,0,0\ldots,0} &= 0\\
a_{0,d-1,1,0,\ldots,0} &= 0\\
a_{0,d-1,0,1\ldots,0} &= 0\\
\vdots &= \vdots\\
a_{0,d-1,0,0\ldots,1} &= 0
\end{aligned}$$

If p is not a divisor of d this amounts to $2(m+1)$ independent conditions provided $d \geq 3$. By the lemma below this proves that the two tangent spaces T_P and T_Q generate a linear subspace in $\mathbb{P}^M$ of dimension $2(m+1)-1 = 2m+1$ and their intersection is empty. If $d = 2$ the number of independent conditions is one less, namely $2(m+1)-1$. Therefore the two tangent spaces T_P and T_Q generate a linear subspace in $\mathbb{P}^M$ of dimension $2(m+1) - 1 - 1 = 2m$ and their intersection is exactly one point.

Likewise, if p is a divisor of d the number of independent conditions is $2m$ and by the lemma below the two tangent spaces T_P and T_Q generate a linear subspace in $\mathbb{P}^M$ of dimension $2m-1$ and their intersection is of dimension one. ∎

Lemma 4. *Let* $\mathbb{P}^M$ *with* $M \geq 1$ *be the projective* M*-space over* k *and let* $\mathbb{P}^{\mathbb{M}^\vee}$ *be the dual projective space of hyperplanes in* $\mathbb{P}^M$. *Let* $L \subseteq \mathbb{P}^M$ *be a linear subvariety. The requirement that the hyperplane* H *contains the linear space* L *imposes* $\dim L + 1$ *linearly independent conditions on* H, *specifically*

$$\dim\{H \in \mathbb{P}^{\mathbb{M}^\vee} \mid L \subseteq H\} = M - (\dim L + 1) \ .$$

Proof: Let $L' \subseteq \mathbb{P}^M$ be a linear subspace disjoint from L of maximal dimension $\dim L' = M - (\dim L + 1)$. Then $H \mapsto H \cap L'$ gives a 1-1 correspondance between hyperplanes H containing the linear space L and the hyperplanes in L'. The hyperplanes in L' is the dual variety $L'^\vee$ of L' and is of dimension $\dim L' = M - (\dim L + 1)$. ∎

References

[1] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[2] R. Hartshorne, *Algebraic geometry*. New York: Springer-Verlag, 1977, graduate Texts in Mathematics, No. 52.

[3] P. A. Chou, Y. Wu, K. Jain, and K. Jain, "Practical network coding," 2003.

[4] T. Ho, M. Mdard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE TRANS. INFORM. THEORY*, vol. 52, no. 10, pp. 4413–4430, 2006.